

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229451

(43)Date of publication of application : 14.08.2002

(51)Int.Cl.

G09C 1/00

G06F 12/14

G06F 17/21

H04L 9/32

(21)Application number : 2001-027130

(71)Applicant : CASIO COMPUT CO LTD

(22)Date of filing : 02.02.2001

(72)Inventor : IIZUKA NORIO

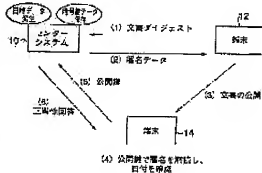
(54) SYSTEM, METHOD, AND PROGRAM FOR GUARANTEEING DATE AND HOUR OF CREATION OF DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To guarantee the date and hour of creation of data.

SOLUTION: When a center system 10 receives the guarantee request of the date and hour of the creation of a document, and a document digest subject to the guarantee from a terminal 12 (1), the center system 10 creates date and hour data, integrates them in a form indivisible from the document digest, creates signature data in which the date and hour data are encrypted on the basis of secret key data by a public key cryptosystem, and transmits them to the terminal 12 (2).

When the terminal 12 publishes the document to a terminal 14, the terminal 12 attaches the signature data and public key data to document data and transmits them. When the center system 10 receives the public key data together with the guarantee request of the validity from the terminal 14 (5), the center system 10 discriminates whether or not the public key data is valid data corresponding to the secret key data used when the creating signature data from the document digest received from the terminal 12, and transmits the discrimination result to the terminal 14 which is the sender of the public key data (6).



(43) 公開日 平成14年8月14日 (2002.8.14)

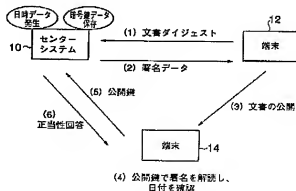
(51) Int.Cl. ⁷	識別記号	F i	テマコード ⁷ (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 5 B 0 0 9
			6 4 0 B 5 B 0 1 7
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 Z 5 J 1 0 4
	3 2 0		3 2 0 A
17/21	5 9 0	17/21	5 9 0 J
審査請求 未請求 請求項の数15 O L (全 16 頁) 最終頁に続く			
(21) 出願番号	特願2001-27130 (P2001-27130)	(71) 出願人	000001443 カシオ計算機株式会社 東京都渋谷区本町1丁目6番2号
(22) 出願日	平成13年2月2日 (2001.2.2)	(72) 発明者	飯塚 宜男 東京都羽村市栄町3丁目2番1号 カシオ 計算機株式会社羽村技術センター内
		(74) 代理人	100058479 弁理士 鈴江 武彦 (外5名) Pターム (参考) 5B009 TB13 VA03 5B017 AA08 BA07 5J104 AA09 LA03 LA05 LA06 MA02 MA02 PA07

(54) 【発明の名称】 データ作成日時保証システム、データ作成日時保証方法、及びデータ作成日時保証プログラム

(57) 【要約】

【課題】 データの作成日時を保証できるようにする。

【解決手段】 センターシステム 10 は、端末 12 より文書の作成日時の保証依頼と保証対象とする文書ダイジェストを受信すると (1)、日時データを作成して文書ダイジェストと不可分な形で統合し、これを公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成して端末 12 に送信する (2)。端末 12 は、端末 14 に対して文書を公開する場合には、文書データに署名データと公開鍵データとを添付して送信する。センターシステム 10 は、端末 14 から公開鍵データと共に正当性の保証依頼を受信すると (5)、端末 12 から受信した文書ダイジェストから署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別し、その判別結果を公開鍵データの送信元である端末 14 に送信する (6)。



【特許請求の範囲】

【請求項1】 端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、

日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データ生成手段によって生成された署名データを前記データ受信手段によって受信したデータの送信元に送信するデータ送信手段とを具備したことを特徴とするデータ作成日時保証システム。

【請求項2】 公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、前記署名データ生成手段によって署名データを生成する際に用いた秘密鍵データに対応する正当なものであることを判断する正当性判断手段と、前記正当性判断手段による判断結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判断結果送信手段とを具備したことを特徴とする請求項1記載のデータ作成日時保証システム。

【請求項3】 端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データ生成手段によって生成された署名データを格納する署名データ格納手段と、前記署名データ格納手段によって格納された署名データを特定するためのリンク情報を前記データ受信手段によって受信したデータの送信元に送信するリンク情報送信手段とを具備したことを特徴とするデータ作成日時保証システム。

【請求項4】 前記署名データ格納手段によって格納された署名データを特定するためのリンク情報と前記署名データ生成手段による署名データの作成対象となつたというデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、前記データ保証依頼受信手段によって受信したデータが前記署名データ生成手段による署名データの生成の対象となつた正当なものであるかを、前記データ保証依頼受信手段により受信した前記リンク情報が示す前記署名

データ格納手段に格納された署名データをもとに判断する正当性判断手段と、

前記正当性判断手段による判断結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判断結果送信手段とを具備したことを特徴とする請求項3記載のデータ作成日時保証システム。

【請求項5】 端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末より日時データの要求を受信する要求受信手段と、日時データを作成する日時データ作成手段と、前記要求受信手段により受信した要求に応じて、前記日時データ作成手段によって作成された日時データを前記要求受信手段によって受信した要求の送信元に送信する日時データ送信手段とを具備したことを特徴とするデータ作成日時保証システム。

【請求項6】 公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、端末において作成されたデータを暗号化する際に用いられる書き換え不能な記録媒体に記録された公開鍵暗号方式による秘密鍵データに対応する正当なものであるかを判断する正当性判断手段と、前記正当性判断手段による判断結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判断結果送信手段とを具備したことを特徴とする請求項5記載のデータ作成日時保証システム。

【請求項7】 データを作成する端末において、作成したデータの作成日時の保証要求を入力する要求入力手段と、

前記要求入力手段によって保証要求が入力された場合に、日時データの要求を所定のシステムに対して送信する要求送信手段と、

前記要求送信手段による要求に対する前記システムからの日時データを受信する日時データ受信手段と、暗号化プログラムと公開鍵暗号方式による秘密鍵データとが記録された記録内容を書き換え不能な記録媒体を用い、作成したデータと前記日時データ受信手段によって受信した日時データとを統合し、前記記録媒体に記録された秘密鍵データをもとに前記暗号化プログラムに従って暗号化した署名データを生成する署名データ生成手段とを具備したことを特徴とする端末。

【請求項8】 再現性のない事象をもとにした付加データを作成する付加データ作成手段と、前記付加データ作成手段によって作成された付加データを前記日時データ作成手段によって作成された日時データと対応づけて格納する付加日時データ格納手段とを具備し、

前記日時データ送信手段は、前記日時データと共に前記付加データ作成手段によって作成された付加データを送

3

信することを特徴とする請求項5記載のデータ作成日時保証システム。

【請求項9】 日時データと付加データと共に、これらのデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、

前記データ保証依頼受信手段によって受信した日時データと付加データとが正当なものであるかを、前記付加日時データ格納手段に格納された日時データと付加データとをもとに判別する付加日時データ正当性判別手段と、前記付加日時判別データ正当性判別手段による判別結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判別結果送信手段とを具備したことを特徴とする請求項8記載のデータ作成日時保証システム。

【請求項10】 端末において作成されたデータの作成日時を保証するデータ作成日時保証方法であって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信ステップと、

日時データを作成する日時データ作成ステップと、前記データ受信ステップによって受信したデータと前記日時データ作成ステップによって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成ステップと、

前記署名データ生成ステップによって生成された署名データを前記データ受信ステップによって受信したデータの送信元に送信するデータ送信ステップと、公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信ステップと、

前記公開鍵データ保証依頼受信ステップによって受信した公開鍵データが、前記署名データ生成ステップによって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別ステップと、

前記正当性判別ステップによる判別結果を、前記公開鍵データ保証依頼受信ステップにより受信した公開鍵データの送信元に送信する判別結果送信ステップとを有することを特徴とするデータ作成日時保証方法。

【請求項11】 端末において作成されたデータの作成日時を保証するためにコンピュータを、

端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、

日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データ生成手段によって生成された署名データを前記データ受信手段によって受信したデータの送信元

に送信するデータ送信手段と、公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、

前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、前記署名データ生成手段によって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とに機能させるためのデータ作成日時保証プログラム。

【請求項12】 端末において作成されたデータの作成日時を保証するデータ作成日時保証方法であって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信ステップと、

日時データを作成する日時データ作成ステップと、前記データ受信ステップによって受信したデータと前記日時データ作成ステップによって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成ステップと、

前記署名データ生成ステップによって生成された署名データを格納する署名データ格納ステップと、前記署名データ格納ステップによって格納された署名データを特定するためのリンク情報を前記データ受信ステップによって受信したデータの送信元に送信するリンク情報送信ステップと、

前記署名データ格納ステップによって格納された署名データを特定するためのリンク情報と前記署名データ生成ステップによる署名データの作成対象となつていてデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信ステップと、

前記データ保証依頼受信ステップによって受信したデータが前記署名データ生成ステップによる署名データの生成の対象となつた正当なものであるかを、前記データ保証依頼受信ステップにより受信した前記リンク情報が示す前記署名データ格納ステップに格納された署名データをもとに判別する正当性判別ステップと、

前記正当性判別ステップによる判別結果を、前記データ保証依頼受信ステップによって受信したデータの送信元に送信する判別結果送信ステップとを有することを特徴とするデータ作成日時保証方法。

【請求項13】 端末において作成されたデータの作成日時を保証するためにコンピュータを、

端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、

日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合

し、公開鍵暗号方式による秘密鍵データをもとに暗号化
した署名データを生成する署名データ生成手段と、
前記署名データ生成手段によって生成された署名データ
を格納する署名データ格納手段と、

前記署名データ格納手段によって格納された署名データ
を特定するためのリンク情報を前記データ受信手段によ
って受信したデータの送信元に送信するリンク情報送信
手段と、

前記署名データ格納手段によって格納された署名データ
を特定するためのリンク情報と前記署名データ生成手段
による署名データの作成対象となつたとしているデータ
と共に、このデータに関する正当性の保証依頼を受信す
るデータ保証依頼受信手段と、

前記データ保証依頼受信手段によって受信したデータが
前記署名データ生成手段による署名データの生成の対
象となつた正当なものであるかを、前記データ保証依頼
受信手段により受信した前記リンク情報が示す前記署名
データ格納手段に格納された署名データをもとに判別す
る正当性判別手段と、

前記正当性判別手段による判別結果を、前記データ保証
依頼受信手段によって受信したデータの送信元に送信す
る判別結果送信手段とに機能させるためのデータ作成日
時保証プログラム。

【請求項14】 端末において作成されたデータの作成
日時を保証するデータ作成日時保証方法であつて、
端末より日時データの要求を受信する要求受信ステッ
プと、

日時データを作成する日時データ作成ステップと、
前記要求受信ステップにより受信した要求に応じて、前
記日時データ作成ステップによって作成された日時データ
を前記要求受信ステップによって受信した要求の送信
元に送信する日時データ送信ステップと、
公開鍵暗号方式による公開鍵データと共に、この公開鍵
データに関する正当性の保証依頼を受信する公開鍵データ
保証依頼受信ステップと、

前記公開鍵データ保証依頼受信ステップによって受信し
た公開鍵データが、端末において作成されたデータを暗
号化する際に用いられる書き換え不能な記録媒体に記録
された公開鍵暗号方式による秘密鍵データに対応する正
当なものであるかを判別する正当性判別ステップと、
前記正当性判別ステップによる判別結果を、前記公開鍵
データ保証依頼受信ステップによって受信した公開鍵データ
の送信元に送信する判別結果送信ステップとを有する
ことを特徴とするデータ作成日時保証方法。

【請求項15】 端末において作成されたデータの作成
日時を保証するためにコンピュータを、

端末より日時データの要求を受信する要求受信手段と、
日時データを作成する日時データ作成手段と、
前記要求受信手段により受信した要求に応じて、前記日
時データ作成手段によって作成された日時データを前記

要求受信手段によって受信した要求の送信元に送信する
日時データ送信手段と、

公開鍵暗号方式による公開鍵データと共に、この公開鍵
データに関する正当性の保証依頼を受信する公開鍵データ
保証依頼受信手段と、

前記公開鍵データ保証依頼受信手段によって受信した公
開鍵データが、端末において作成されたデータを暗号化
する際に用いられる書き換え不能な記録媒体に記録され
た公開鍵暗号方式による秘密鍵データに対応する正当な
ものであるかを判別する正当性判別手段と、

前記正当性判別手段による判別結果を、前記公開鍵データ
保証依頼受信手段によって受信した公開鍵データの送信
元に送信する判別結果送信手段とに機能させるための
データ作成日時保証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、端末において作成
されたデータの日時を保証するデータ作成日時保証シス
テム、データ作成日時保証方法、及びデータ作成日時保
証プログラムに関する。

【0002】

【従来の技術】近年、インターネットなどのネットワ
ークの発達に伴い、ネットワークを介して様々なデータが
コンピュータ間で送受信されている。重要なデータにつ
いては、データの正当性を証明するためのデジタル署名
の技術が用いられており、生成されたデータの改ざん防
止が図られている。

【0003】デジタル署名は、データの送信者は、送信
対象とするデータをもとにして公開鍵暗号方式における
秘密鍵（かぎ）を用いて署名データを作成し、この署名
データを送信対象とするデータに付けて送信する。受信
者は、公開鍵を使って署名データを復号し、この復号化
された署名データと受信したデータをもとにして、署
名データが正しい送信者が署名したものであり、データ
が改ざんされていないことを確認できる。

【0004】また、公開鍵が正当であることを保証する
ために認証局という機関が設けられている。認証局は、
公開鍵暗号方式に基づくデジタル署名を利用するときの
公開鍵が正当であることを保証する証明書を発行する。
受信者は、発信者が配布した公開鍵が認証局からの証明
書付きであれば、公開鍵についても正当であることを確
認することができる。

【0005】

【発明が解決しようとする課題】しかしながら、従来の
デジタル署名の技術は、データの作成者とデータの正当
性を保証するものであつて、データの作成日時を保証す
ることができなかった。例えば特許出願しようとする開
発技術に関して文書を作成した場合、文書作成時には非
公開であるが、何れ公開する際に作成日時を保証でき
るようにしておきたいという要求がある。しかし、従来の

デジタル署名の技術では文書の内容が改ざんされていないという正当性を保証できても、文書の作成日時については保証することができなかった。

【0006】通常、パーソナルコンピュータなどにおいてデータを作成した場合には、そのデータのファイルについてデータ更新日時を表すタイムスタンプが記憶されるが、コンピュータに搭載された時計が正確ではないことがあり、またファイルスタンプに対する変更が容易にできるために、精度と信頼性について満足できるものではなかった。

【0007】本発明は、前記のような問題に鑑みなされたもので、データの作成日時を保証することができるデータ作成日時保証システム、データ作成日時保証方法、及びデータ作成日時保証プログラムを提供することを目的とする。

【0008】

【課題を解決するための手段】本発明は、端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データ生成手段によって生成された署名データを前記データ受信手段によって受信したデータの送信元に送信するデータ送信手段とを具備する。

【0009】また、公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、前記署名データ生成手段によって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とを具備したことを特徴とする。

【0010】また本発明は、端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データの署名データ格納手段と、前記署名データ格納手段によって格納された署名データを特定するためのリンク情報を前記データ受信手

段によって受信したデータの送信元に送信するリンク情報送信手段とを具備したことを特徴とする。

【0011】また、前記署名データ格納手段によって格納された署名データを特定するためのリンク情報と前記署名データ生成手段による署名データの作成対象となったとしているデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、前記データ保証依頼受信手段によって受信したデータが前記署名データ生成手段による署名データの生成の対象となった正当なものであるかを、前記データ保証依頼受信手段により受信した前記リンク情報が示す前記署名データ格納手段に格納された署名データをもとに判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判別結果送信手段とを具備したことを特徴とする。

【0012】また本発明は、端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末より日時データの要求を受信する要求受信手段と、日時データを作成する日時データ作成手段と、前記要求受信手段により受信した要求に応じて、前記日時データ作成手段によって作成された日時データを前記要求受信手段によって受信した要求の送信元に送信する日時データ送信手段とを具備したことを特徴とする。

【0013】また、公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、端末において作成されたデータを暗号化する際に用いられる書き換え不能な記憶媒体に記録された公開鍵暗号方式による秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とを具備したことを特徴とする。

【0014】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について説明する。図1は、第1乃至第3実施形態におけるシステムの構成を示すブロック図である。図1に示すように、センタシステム10（データ作成日時保証システム）は、インターネット、公衆回線網などの各種通信系を含むネットワーク11を介して、一般ユーザが使用する端末12、14、端末12、14を使用するユーザが口座を開設している銀行の銀行サーバ16と接続される。

【0015】センタシステム10は、データ作成日時保証サービスを提供するもので、端末12、14において作成されたデータに対して、自システム内で発生させた日時データをもとにデータ作成日時が保証されるよう

にする。センタースystem 10は、端末 12、14に対してデータ作成日時保証サービスの提供することで課金を行ない、端末 12、14のユーザが口座を開設している銀行の銀行サーバ 16より課金料金を徴収する。

【0016】端末 12、14は、一般のユーザによって使用されるもので、ユーザからの指示に応じてアプリケーションプログラムにより各種処理を実行する。図 1では、端末 12において、アプリケーションプログラムによりデータを作成し、このデータに対するデータ作成日時の証明をセンタースystem 10に依頼するものとし、端末 14において、端末 12で作成されたデータについて、その作成日時を確認するものとして説明する。

【0017】銀行サーバ 16は、端末 12、14のユーザが開設している銀行口座を持つ銀行のサーバであり、ネットワーク 11を通じて受信した指示に応じて銀行口座に対する操作を行うことができる。

【0018】図 1中に示すセンタースystem 10、端末 12、14、銀行サーバ 16は、各種の記録媒体に記録されたプログラムを読み込み、その読み込んだプログラムによって動作が制御されるコンピュータによって構成される。例えば、端末 12、14は、パーソナルコンピュータ、PDA (personal digital assistant)、携帯電話などの個人ユーザにより使用されるように構成されたもので、センタースystem 10は、サーバシステム等の比較的大規模に構成されたものである。

【0019】図 1にはセンタースystem 10の主要な構成部分のみを示している。図 1に示すように、センタースystem 10は、CPU 20が記憶部 21、通信部 22、及び時計部 23と相互に接続されている。

【0020】CPU 20は、センタースystem 10全体の制御を司るもので、記憶部 21に記録されたプログラムを実行することにより各種の処理を実行する。CPU 20は、記憶部 21に記録された日時保証サービスプログラム 21aを実行することにより、端末 12が作成したデータについて作成日時を保証するためのデータ作成日時保証サービスを実行する。

【0021】記憶部 21は、CPU 20によってアクセスされるプログラムやデータの情報が記録されるもので、本実施形態では例えば日時保証サービスプログラム 21aなどの各種プログラムや、各プログラムを実行する際に用いられる各種データの他、作業用のデータを一時的に記録するためのワークエリアなどが設定される。

日時保証サービスプログラム 21aの実行に伴って格納される各種データとしては、公開鍵暗号方式による暗号化に用いる暗号鍵データ 21b (秘密鍵データ)、暗号鍵データ 21bを用いた暗号化の処理対象となる処理データ 21c (第 1及び第 2実施形態では文書データ (文書ダイジェスト)、第 3実施形態では日時データ)、データ作成日時保証サービスを提供したことに對するユーザへの課金に関する課金データ 21dなどが含まれてい

る。

【0022】記憶部 21は、記憶媒体を有しており、記憶媒体に対するプログラム、データ等の記録や読み出しを実行する。記憶媒体は磁気的、光学的記録媒体、もしくは半導体メモリで構成され、記憶部 21に固定的に設けたもの、もしくは着脱自在に装着するものである。また、記憶媒体に記録されるプログラム、データ等は、通信回路等を介して接続された他の機器から受信して記録する構成にしても良く、さらに、通信回路等を介して接続された他の機器側に記録媒体を備えた記録装置を設け、この記録媒体に記録されているプログラムやデータを、通信回路を介して使用する構成にしても良い。記憶部 21は、記憶媒体に対して各種アプリケーションによって使用される各種のデータ等も記録し、必要に応じて読み出して利用することができる。

【0023】通信部 22は、CPU 20の制御のもとでネットワーク 11を介した他の電子機器 (端末 12、14、銀行サーバ 16など) との通信を制御する。時計部 23は、年月日時時刻を表す日時データを発生して CPU 20に提供する。時計部 23は、例えばセンタースystem 10の動作と関係なく正確な日時データを発生することができるよう特別なハードウェアによって構成されているものとする。

【0024】また、図 1には端末 12の主要な構成部分のみを示している。図 1に示すように、端末 12は、CPU 30が記憶部 31、通信部 32、入力部 33、及び表示部 34と相互に接続されている。

【0025】CPU 30は、端末 12全体の制御を司るもので、記憶部 31に記録されたプログラムを実行することにより各種の処理を実行する。CPU 30は、記憶部 31に記録されたアプリケーションプログラム 31bを実行することにより、このアプリケーションに用いられるデータを作成する。以下の説明では、アプリケーションプログラム 31bが文書作成用プログラムであり、文書データを作成するものとして説明する。また、CPU 30は、日時保証サービスプログラム 31aを実行することにより、例えばアプリケーションプログラム 31bによって作成されたデータについての作成日時の保証要求がユーザから指示された場合に、センタースystem 10が提供するデータ作成日時保証サービスを利用してデータ作成日時が保証されるようにする処理を実行する。

【0026】記憶部 31は、CPU 30によってアクセスされるプログラムやデータの情報が記録されるもので、本実施形態では例えば日時保証サービスプログラム 31a、アプリケーションプログラム 31bなどの各種プログラムや、各プログラムを実行する際に用いられる各種データの他、作業用のデータを一時的に記録するためのワークエリアなどが設定される。

【0027】記憶部 31は、記憶媒体を有しており、記

12

10

20

30

40

50

【0032】CPU30は、文書ダイジェストを作成すると、通信部32からネットワーク11を通じて、センターシステム10に対してデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを送信する（ステップA4、図2（1））。

【0304】そして、GPU20は、時計部23から取得した日時データと、端末2から取得した文書データベースとを不可分な形で統合し、この統合したデータを予めセンターシステム10において用意されている暗号化データ21bに含まれる公開暗号方式による秘密鍵データを用いて、所定の暗号化アルゴリズムに従って暗号化して署名データを生成する（ステップB3）。センターシステム10において用意されている暗号化データ21b（秘密鍵データ）は、センター側でユーザによって取得されないよう管理されている。

【0036】また、センターシステム10は、端末12のユーザへの課金に関する課金データ21dを設定して記憶する。センターシステム10は、例えば予め設定された期間毎（月末毎など）に、各ユーザについて設定されている課金データ21dに基づいて端末12のユーザが開設している口座を持つ銀行の銀行サーバ16にアクセスして、所定の課金金額を徴収する。なお、センターシステム10は、サービス料を課金する場合には、データ作成日時保証サービスを利用するユーザに対して、予めユーザに関する情報（氏名、課金口座、連絡先など）を登録しておくものとする。そして、ユーザに関する情報の登録時各ユーザに対してデータ作成日時保証サービスを利用する際のパスワードなどを発行しておき、このパスワードで利用時に指定させることで、課金対象とするユーザ（課金口座）を識別するものとする。

【0037】一方、端末12は、センタシステム10から署名データと公開鍵データを受信すると、作成した文書データと対応づけて記憶しておく。そして、文書データを外部に公開する場合（図2（3））、例えば端末14のユーザにネットワーク11を通じて提供する場合には、文書データに署名データと公開鍵データとを添

13

付して送信する（ステップA5）。

【0038】なお、前述した説明では、端末12からセンターシステム10に対してハッシュ関数等を用いて作成された文書ダイジェストを送信するものとしているが、端末12において作成された文書データの全てをセンターシステム10に送信して、センターシステム10において文書データを文書ダイジェスト化するようにしても良い。

【0039】また、端末12において文書データ作成時に、センターシステム10が提供するデータ作成日時保証サービスを利用して作成日時の保証を得るものとしているが、文書データを作成した後、例えばユーザからの指示に応じて実行するようにしても良い。基本的には、データ作成時と同時に作成日時の保証を受ける方が望ましいが、任意のタイミングで作成日時の保証を受けたとしても、少なくともその日時保証を受けた日時以前に文書が作成されたことを保証することができる。

【0040】こうして、端末12において作成された文書データについて、センターシステム10が提供するデータ作成日時保証サービスを利用して、文書データの作成日時を保証するための署名データを文書データに添付して公開することができる。

【0041】次に、端末14において、端末12により公開された文書データの作成日時を確認しようとする場合について、図4に示すフローチャートを参照しながら説明する。なお、証明付き公開文書を読むことができるプログラムが一般に公開されており、センターシステム10によるデータ作成日時保証サービスを利用して署名データが添付された文書データについてもこのプログラムによって読むことができるものとする。端末14には、このプログラムが記憶されており、このプログラムを実行することで以下のようにして端末12により公開された署名データが添付された文書データを読むことができる。

【0042】まず、端末14は、端末12により公開された文書データと共に、署名データと公開鍵データとを受信し（ステップa1）、この受信した文書データについての確認指示がユーザにより入力されると、文書データに添付されていた公開鍵データを用いて署名データを解読することによって文書ダイジェストと日時データとを取得する。

【0043】端末14は、文書データに対してハッシュ関数により文書ダイジェストを生成し、この生成した文書ダイジェストと署名データを解読することにより得られた文書ダイジェストとを比較することで、文書データの内容が改ざんされているか否かを確認する。すなわち、両者が同一であれば文書データの内容が改ざんされていないと判別することができる。さらに、端末14は、文書データの内容が改ざんされているか否かの判別結果に応じて、日時データが改ざんされているか否かを

14

確認する（ステップa2、図2（4））。すなわち、署名データは、センターシステム10において、文書ダイジェストと日時データとを統合して暗号化されたデータであるため、署名データを復号化して得た文書データが改ざんされていないければ、日時データについても改ざんされていないことが保証される。従って、端末14のユーザは、保証された日時データによって端末12により公開された文書の作成日時を確認することができる。

【0044】さらに第1実施形態においては、センターシステム10は、端末12により公開された署名データを復号化する際に用いた公開鍵データについての正当性を保証するためのサービスを提供する。これは、センターシステム10における暗号化で用いられる暗号化アルゴリズムが盗まれた場合、改ざんされた文書データあるいは日時データに対して、この暗号化アルゴリズムにより不正な秘密鍵データを用いて暗号化され、この暗号化で用いられた秘密鍵データに対応する公開鍵データが署名データに添付されて公開されてしまうおそれがあるためである。この場合、前述したように署名データに対して、この署名データに添付された公開鍵データによって復号化すると、文書ダイジェストと日時データと共に正当であるかと判定されてしまう。

【0045】端末14は、端末12が公開した署名データに対する公開鍵データの保証依頼と共に、公開鍵データをセンターシステム10に対してネットワーク11を通じて送信する（ステップa3、図2（5））。

【0046】センターシステム10は、端末14から公開鍵データの保証依頼と共に、保証対象とする公開鍵データを受信すると（ステップB6）、この公開鍵データについての正当性を判別するための正当性判別処理を実行する（ステップB7）。正当性判別処理では、保証対象とする公開鍵データが署名データを生成（暗号化）する際に用いた秘密鍵データに対応するものか、すなわちセンターシステム10が管理する秘密鍵データを用いて暗号化したデータを保証対象とする公開鍵データによって復号化した時に正しいデータが得られるか否かによって判別する。

【0047】センターシステム10は、正当性判別処理によって得られた結果を正当性に関する回答として、公開鍵データの保証依頼元である端末14に対して送信する（ステップB8、図2（6））。

【0048】端末14は、センターシステム10から正当性回答を受信し、公開鍵データが正当であるか否かを確認することができる（ステップa4）。

【0049】このようにして、第1実施形態のセンターシステム10は、端末12において作成された文書データ（文書ダイジェスト）に対して、センターシステム10において生成した信頼性の高い日時データを不可分形で統合して、ユーザにより取得できない秘密鍵データを用いて暗号化するため、文書データと日時データの両

15
方について、第3者だけでなく文書の作成者によっても改ざんすることができないため、文書の作成が日時データにより示される日時（少なくともそれ以前）に行われたことを文書作成後であっても保証することができる。また、公開鍵暗号方式による公開鍵データを用いて日時データの検証をすることができるので、何時でも誰によっても文書の作成日時を確認することができる。

【0050】なお、前述した説明では、データ作成日時保証サービスによる保証の対象が文書データと日時データであるとしているが、文書の作成者を表す作成者データを保証対象に含めるようにしても良い。この場合、センタースystem 10では、文書ダイジェストと日時データと作成者データとを統合して暗号化し、この暗号化により得られた作成者データを含む署名データを端末12に送信する。以下、作成者データについても日付データと同様に処理することで、文書データの作成日時と共に文書の作成者についても保証することができる。

【0051】また、端末12からは文書全体を公開するものとしているが、作成文書の抄録などを作成日時の保証を付けて公開することで、文書全体を秘匿した状態で、文書が作成されたことについて証明することもできる。

【0052】次に、本発明の第2実施形態の動作について説明する。図5は第2実施形態におけるセンタースystem 10が提供するデータ作成日時保証サービスの概略を説明するための図、図6はセンタースystem 10において管理される署名データベース10a（後述する）に登録されるデータの一例を示す図、図7（a）（b）はセンタースystem 10と端末12における動作を説明するためのフローチャート、図8（a）（b）はセンタースystem 10と端末14における動作を説明するためのフローチャートである。

【0053】なお、図7（a）のフローチャートに示すステップC1～C4の処理については、前述した図3（a）のフローチャートに示すステップA1～A4の処理と同様にして実行されるものとして詳細な説明を省略する。

【0054】端末12により文書が作成され、日時証明の操作がなされると、CPU30は、文書ダイジェストを作成し、通信部32からネットワーク11を通じて、センタースystem 10に対してデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを送信する（ステップC4、図5（1））。

【0055】一方、センタースystem 10のCPU20は、日時保証サービスプログラム21aに基づいて、通信部22によって端末12からデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを受信すると、処理データ21cとして一時的に記憶部21bに格納すると共に（ステップD1）、時刻部23によって発生される現在の年月日時刻を表す日時データを取得する（ス

ップD2）。

【0056】そして、CPU20は、時計部23から取得した日時データと、端末12から取得した文書ダイジェストとを不可分な形で統合し、この統合したデータを予めセンタースystem 10において用意されている暗号鍵データ21bに含まれる公開鍵暗号方式による秘密鍵データを用いて、所定の暗号化アルゴリズムに従って暗号化して署名データを生成する（ステップD3）。センタースystem 10において用意されている暗号鍵データ21b（秘密鍵データ）は、センタースystem 10によって取得されないよう管理されている。

【0057】センタースystem 10は、秘密鍵データをもとに暗号化して得られた署名データと、この暗号化に用いた秘密鍵データ（暗号化鍵データ）とを対応づけて署名データベース10aとして記憶部21に登録すると共に、これらの情報を特定するためのリンク情報も対応付けて登録する。そして、センタースystem 10は、署名データベース10aに登録したリンク情報のみを端末12に送信する（ステップD4、図5（2））。

【0058】また、センタースystem 10は、端末12のユーザへの課金に関する課金データ21dを設定して記憶する（ステップD5）。なお、課金に関しては第1実施形態と同様にして行われるものとして詳細な説明を省略する。

【0059】一方、端末12は、センタースystem 10からリンク情報を受信すると、作成した文書データと対応づけて記憶しておく。そして、文書データを外部に公開する場合、例えば端末14のユーザにネットワーク11を通じて提供する場合には、文書データにリンク情報を添付して送信する（ステップC5）。

【0060】こうして、端末12において作成された文書データについて、センタースystem 10が提供するデータ作成日時保証サービスを利用して、文書データの作成日時を保証するための署名データをセンタースystem 10の署名データベース10aに登録しておくことができる。従って、センタースystem 10に作成文書の保証依頼をした後では、端末12のユーザであっても文書内容、作成日付を変更することができない。また、センタースystem 10から端末12に対してはリンク情報のみを送信するので通信に要するコストを低減することができる。

【0061】次に、端末14において、端末12により公開された文書データの作成日時を確認しようとする場合について、図8（a）（b）に示すフローチャートを参照しながら説明する。なお、第2実施形態においても、端末14には証明付き公開文書を読むことができるプログラムが記憶されており、このプログラムを実行することで以下のようにして端末12により公開された文書データを読むことができると共にセンタースystem 10において管理されている文書の作成日を示す日付データ

の確認ができるものとする。

【0062】まず、端末14は、端末12により公開された文書データと共にリンク情報を受信し（ステップc1）、この受信した文書データについての確認指示がユーザにより入力されると、文書データに対してハッシュ関数により文書ダイジェストを生成し、端末12が公開した文書の保証依頼と共に生成した文書ダイジェストとリンク情報とをセンターシステム10に対してネットワーク11を通じて送信する（ステップc2、図5（4））。

【0063】第2実施形態においては、センターシステム10は、端末12により公開された文書に添付されたリンク情報をもとに、署名データベース10aにおいて管理している署名データを特定し、この特定された署名データをもとに文書の正当性を保証すると共に文書の作成日時を確認するためのサービスを提供する。

【0064】センターシステム10は、端末14から文書の保証依頼と共に、保証対象とする文書の文書ダイジェストとリンク情報を受信すると（ステップD6）、文書と日付データについての正当性を判断するための正当性判断処理を実行する（ステップD7）。正当性判断処理では、端末14から受信したリンク情報をもとに、署名データベース10aに登録されたリンク情報が示す署名データを特定する。そして、特定した署名データと対応して登録された秘密鍵データ（暗号化鍵データ）に対応する公開鍵データを用いて署名データを復号化（解読）し、文書ダイジェストと日付データとを生成する。センターシステム10は、復号化によって生成した文書ダイジェストと端末14から受信した文書ダイジェストとを比較することによって、端末12により公開された文書（端末14からの文書ダイジェスト）が正当であるかを判断する。すなわち、文書ダイジェストが一致する場合には、端末12により生成されてセンターシステム10により作成日時保証を受けた文書が改ざんされることなく公開されたものと判断できる。また、文書ダイジェストが一致することで、復号化により生成された日付データも正当であり、この日付データが示す日時（少なくともそれ以前）に文書が作成されたことを確認することができる。

【0065】センターシステム10は、正当性判断処理によって得られた結果を正当性に関する回答として、公開鍵データの保証依頼元である端末14に対して送信する（ステップD8、図5（6））。文書内容が正当（改ざんされていない）と判断された場合には、センターシステム10は、日時データも端末14に対して送信する。

【0066】端末14は、センターシステム10から正当性回答を受信し、文書内容が正当であるかを確認し、正当である場合には文書作成日時を示す日時データを受信することができる（ステップc3）。

【0067】このようにして、第2実施形態のセンターシステム10は、端末12において作成された文書データ（文書ダイジェスト）に対して、センターシステム10において生成した信頼性の高い日時データを不可分な形で統合して、ユーザにより取得できない秘密鍵データを用いて暗号化し、署名データベース10aにおいて登録して管理するので、文書データと日時データの両方について、第三者だけでなく文書の作成者によっても改ざんすることができず、文書の作成が日時データにより示される日時（少なくともそれ以前）に行われたことを文書作成後であっても保証することができる。また、端末12、14では、センターシステム10によるデータ作成日時保証サービスを利用することにより得た文書に対するリンク情報のみを保持していれば、任意に作成文書の内容の正当性と作成日時の確認を行うことができるので管理を容易にすることができる。

【0068】なお、前述した説明では、データ作成日時保証サービスによる保証の対象が文書データと日時データであるとしているが、第1実施形態と同様にして、文書の作成者を表す作成者データを保証対象に含めるようにしても良い。

【0069】次に、本発明の第3実施形態の動作について説明する。図9は第3実施形態におけるセンターシステム10が提供するデータ作成日時保証サービスの概略を説明するための図、図10は（a）（b）はセンターシステム10と端末12における動作を説明するためのフローチャートである。

【0070】第3実施形態では、センターシステム10が提供するデータ作成日時保証サービスを利用して、端末12において作成した文書についての作成日時保証を受けるためには、センターシステム10の例えば管理者が配布するICカード40が用いられる。ICカード40は、所定の暗号化プログラム41と、この暗号化プログラム41による暗号化で使用される公開鍵データ方式による秘密鍵データ42とが記録された記録内容を書き換え不能な記録媒体であり、端末12に装着されることで使用される。

【0071】まず、端末12は、アプリケーションプログラム31bによって、ユーザからの指示に応じて文書データを作成したものとする（ステップE1）。端末12を使用するユーザは、作成した文書について作成日時の証明が欲しい場合には、所定の操作により入力部33から作成日時の証明要求を入力する（ステップE2）。

【0072】CPU30は、所定の操作によって作成日時の証明要求が入力されると、日時保証サービスプログラム31aを起動し、このプログラムに従う処理を実行する。まず、CPU30は、作成日時の証明対象とする元文書データについて第1実施形態と同様にして文書ダイジェストを作成する（ステップE3）。

【0073】CPU30は、文書ダイジェストを作成す

ると、通信部32からネットワーク11を通じて、センターシステム10に対して日時データの送信を要求する(ステップE4、図9(1))。

【0074】一方、センターシステム10のCPU20は、日時保証サービスプログラム21aに基づいて、通信部22によって端末12から日時データの送信要求を受信すると(ステップF1)、時計部23によって発生する現在の年月日時刻を表す日時データを取得する(ステップF2)。

【0075】そして、CPU20は、時計部23から取得した日時データに対して、予めセンターシステム10において用意されている暗号鍵データ21bに含まれる公開鍵暗号方式による秘密鍵データを用いて、所定の暗号化アルゴリズムに従って暗号化する(ステップF3)。センターシステム10において用意されている日時データに対する暗号鍵データ21b(秘密鍵データ)は、センター側でユーザによって取得されないよう管理されている。

【0076】センターシステム10は、秘密鍵データをもとに暗号化した日時データを端末12に送信する(ステップF4、図9(2))。

【0077】また、センターシステム10は、端末12のユーザへの課金に関する課金データ21dを設定して記憶する。なお、課金に関しては第1実施形態と同様にして行われるものとして詳細な説明を省略する。

【0078】一方、端末12は、センターシステム10から暗号化された日時データを受信すると(ステップE5)、この暗号化に用いた秘密鍵データに対応する公開鍵暗号方式による公開鍵データを用いて日時データを復号化する。

【0079】そして、端末12は、センターシステム10から取得した日時データと、先に作成した文書ダイジェストとを不可分な形で統合し、この統合したデータをICカード40に記憶された公開鍵暗号方式による秘密鍵データ42を用いて、暗号化プログラム41に従って暗号化して署名データを生成する(ステップE7、図9(3))。

【0080】文書データを外部に公開する場合、例えば端末14のユーザにネットワーク11を通じて提供する場合には、文書データにICカード40を用いて生成した署名データと、ICカード40に格納された秘密鍵データ42に対応する公開鍵データとを添付して送信する(ステップE8、図9(4))。

【0081】なお、前述した説明では、ICカード40に格納された暗号化プログラム41により署名データを生成する処理のみを実行するように説明しているが、端末12のユーザから作成日時の証明要求が入力された以降の処理をユーザからの指示によらず暗号化プログラム41に従って実行するものとしても良い。

【0082】こうして、センターシステム10から取得

した日時データと文書ダイジェストとを統合し、ICカード40を用いて署名データを生成し、端末12において作成された文書データに対して添付して公開することができる。第3実施形態では、ICカード40がなければセンターシステム10から取得した日時データと文書データとを統合した暗号化をすることができないため、ICカード40を有していない第3者が文書データや日時データを改ざんして署名データを生成することができないので、文書データと日時データとの正当性を保証することができる。

【0083】一方、端末14においては、端末12により公開された文書データの作成日時を確認しようとする場合には、ICカード40の暗号化プログラム41と秘密鍵データ42に対応する公開鍵データを用いて署名データを復号化することで、文書の作成日時を確認することができる(図9(5))。なお、第3実施形態における端末14で実行される処理(公開鍵の正当性の確認など(図9(5)(6)))については、第1実施形態と同様にして実行されるものとして詳細な説明を省略する。

【0084】なお、前述した説明では、端末12において署名データを生成するために用いる暗号化プログラム41と秘密鍵データ42とをICカード40によって提供するものとしているが、暗号化プログラム41と秘密鍵データ42とをハードウェア(ファーム)化して端末12に組み込むようにしても良い。暗号化プログラム41と秘密鍵データ42とをハードウェア化することで、ユーザによる処理過程でのデータの改ざんを防止することができる。

【0085】また、前述した説明では、センターシステム10から提供される日時データが端末12からの要求に応じてネットワーク11を通じて送信されるものとしているが、放送局から日時データ放送(または無線帯域通信)などの方式によって一方的に日時データを送出する形態としても良い。この場合、端末12は、日時データ放送を受信する機能が搭載され、この機能により受信した電波から日時データを分離して署名データの生成に利用する。

【0086】次に、第3実施形態に対する改良の一例について説明する。前述した第3実施形態では、ICカード40を用いて端末12において文書データと日時データに対する暗号化(署名データの生成)をしているため、ICカード40が第3者に悪用されれば文書データや日時データに対する改ざんのおそれはないが、ICカード40や暗号化アルゴリズム、秘密鍵データ自体が悪意のある第3者によって盗まれた場合には、その第3者による不正を回避することができなくなってしまう。

【0087】そこで、センターシステム10は、さらに日時データが第3者によって改ざんされていないことを保証するための日時間問い合わせ応答サービスを提供する。

【0088】このために、センタースystem 10は、再現性のない事象をもとにした付加データを作成する機能と、この機能により作成された付加データを端末14に提供する日時データと対応づけて付加日時データベース10bに登録しておく機能が設けられる。図11には付加日時データベース10bに格納されるデータの一例を示している。

【0089】センタースystem 10は、端末12から日時データの送信要求を受信した場合、時計部23によって発生される現在の年月日時時刻を表す日時データを取得すると共に付加データを生成し、この日時データと付加データとを対応づけて付加日時データベース10bに登録しておく。また、日時データと付加データと統合して暗号化し、端末12に暗号化された日時データとして送信する。

【0090】再現性のない事象をもとにした付加データとしては、例えば自然現象や生体現象をもとにしたデータや、機器が発生する誤差を含むデータなどを利用することができる。機器が発生する誤差を含むデータとしては、例えばセンタースystem 10内に設置されたデジタル温度センサーの熱雑音を含めた下位1ビットの50msごとに20回測定した20ビット列のデータ（この場合、1秒に対する付加データ）がある。

【0091】以下、第3実施形態と同様にして、端末12では付加データを含めて署名データを生成して端末14に送信する。

【0092】一方、端末14は、端末12から公開された文書の作成日時を確認するために、公開鍵データの正当性の保証依頼と同様にして、日時データの正当性の保証依頼と共に日時データと付加データとをセンタースystem 10に送信する（図9（5））。

【0093】。

【0094】センタースystem 10は、端末14から日時データと付加データと共に、これらのデータに関する正当性の保証依頼を受信すると、受信した日時データと付加データとが正当なものであるかを、付加日時データベース10bに格納された日時データと付加データとをもとに判断する。すなわち、センタースystem 10は、端末14からの日時データと付加データとの対応関係が付加日時データベース10bに登録されている場合には、日時データが改ざんされていないものと判断することができる。センタースystem 10は、この判断結果を回答として、日時データの保証依頼元である端末14に対して送信する（図9（6））。

【0095】このようにして、日時データに付加された付加データは、センタースystem 10の付加日時データベース10bにおいて管理されているため、端末12において作成された文書の作成日付が万が一改ざんされたとしても、付加日時データベース10bに登録されている日時データと付加データとが一致なくなるため、改

ざんされたことを容易に判断することができる。これにより、日時データに対するセキュリティレベルをより向上させることができる。なお、前述した日時問い合わせ応答サービスは、第3実施形態に限らず第1実施形態、第2実施形態のそれぞれに対して適用することができる。

【0096】また、前述した各実施形態においては、文書作成が行われる端末12のユーザに対して課金を行うものとして説明しているが、データ作成日時保証サービスを利用して端末12において作成された日時を確認する端末14のユーザに対して課金するようにしてもよい。この場合、端末14のユーザに対しても、予めユーザに関する情報（氏名、課金口座、連絡先など）を登録しておくと共にデータ作成日時保証サービスを利用する際のパスワードなどを発行しておき、このパスワードを利用時に指定させることで、課金対象とするユーザ（課金口座）を識別するものとする。

【0097】また、本発明は、前述した実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、前述した実施形態で実行される機能は可能な限り適宜組み合わせる実施してもよい。前述した実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜の組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、効果が得られるものであれば、この構成要件が削除された構成が発明として抽出され得る。

【0098】また、前述した各実施形態において記載した処理は、コンピュータに実行させることのできる日時保証プログラムとして、例えば磁気ディスク（フロッピー（登録商標）ディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリなどの記録媒体に書き込んで各種装置に提供することができる。また、通信媒体により伝送して各種装置に提供することも可能である。データ作成日時保証サービスを提供するサーバ（データ作成日時保証システム）を実現するコンピュータは、記録媒体に記録された日時保証プログラムを読み込み、または通信媒体を介して日時保証プログラムを受信し、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【0099】

【発明の効果】以上のように本発明によれば、端末において作成されたデータ（文書など）について、作成された時点（あるいは作成時以降）に作成日時を保証するデータ作成日時保証サービスを提供することができる。データ作成日時保証サービスでは、端末で生成される日時データではなくデータ作成日時保証システムにおいて生成される正確かつ改ざん不能な日時データが提供されるために十分な精度及び信頼性を確保することができる。

【図面の簡単な説明】

【図 1】第 1 乃至第 3 実施形態におけるシステムの構成を示すブロック図。

【図 2】第 1 実施形態におけるセンタースystem 10 が提供するデータ作成日時保証サービスの概略を説明するための図。

【図 3】センタースystem 10 と端末 12 における動作を説明するためのフローチャート。

【図 4】センタースystem 10 と端末 14 における動作を説明するためのフローチャート。

【図 5】第 2 実施形態におけるセンタースystem 10 が提供するデータ作成日時保証サービスの概略を説明するための図。

【図 6】センタースystem 10 において管理される署名データベース 10a（後述する）に登録されるデータの一例を示す図。

【図 7】センタースystem 10 と端末 12 における動作を説明するためのフローチャート。

【図 8】センタースystem 10 と端末 14 における動作を説明するためのフローチャート。

【図 9】第 3 実施形態におけるセンタースystem 10 が提供するデータ作成日時保証サービスの概略を説明する

ための図。

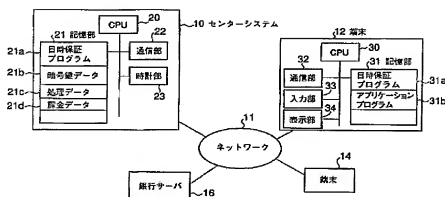
【図 10】センタースystem 10 と端末 12 における動作を説明するためのフローチャート。

【図 11】付加日時データベース 10b に格納されるデータの一例を示す図。

【符号の説明】

10…センタースystem
10a…署名データベース
10b…付加日時データベース
11…ネットワーク
12…端末
12, 14…端末
16…銀行サーバ
20, 30…CPU
21, 31…記憶部
21a, 31a…日時保証プログラム
21b…暗号鍵データ
22, 32…通信部
23…時計部
33…入力部
34…表示部
40…ICカード

【図 1】



【図 6】

10a 署名データベース

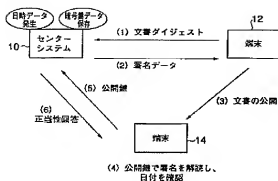
署名データ	暗号化鍵データ	リンク情報

【図 11】

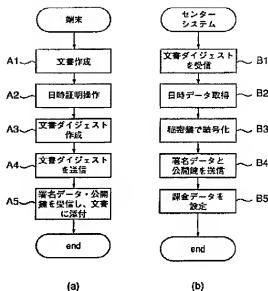
10b 付加日時データベース

付加日時データ	日時データ

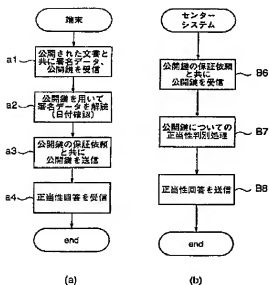
【図2】



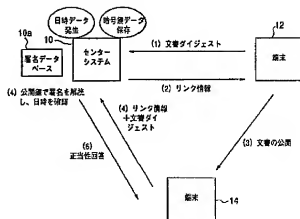
【図3】



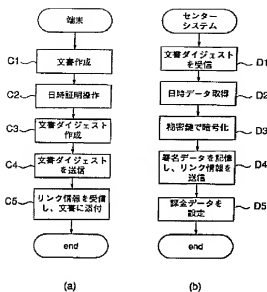
【図4】



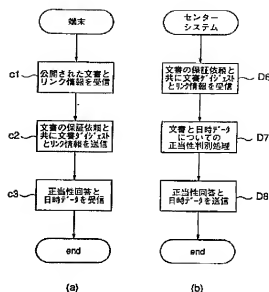
【図5】



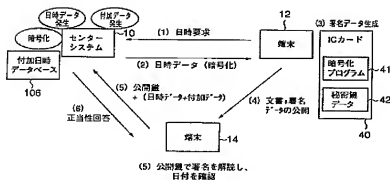
【図 7】



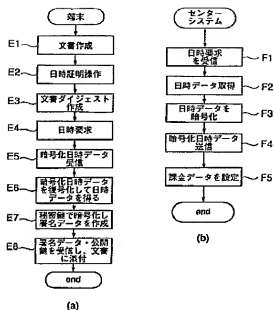
【図 8】



【図 9】



【図 10】



フロントページの続き

(51) Int. Cl.⁷

H04L 9/32

識別記号

FI

H04L 9/00

7-コード* (参考)

673A

675D